https://jdavis.tech/ **Jay Davis, CISM** www.linkedin.com/in/jay-davis
(469) 739-4879

CyberSecurity Specialist

A technology compliance leader and mentor with extensive systems and cyber security experience in cloud and physical environments. Expertise in leading Governance, Risk and Compliance (GRC) teams for Enterprise Solutions through Enterprise Information Risk Management, Security Risk Assessments, Policy, Standards and Application Assessment, Vulnerability and Identity Access Management and IT Auditing.

In-depth knowledge of multiple Security and Regulatory Standards (NIST, HIPAA, SOC, SOX, ISO, PCI-DSS, GDPR, COBIT, OWASP, ITIL, etc.).

Currently finishing a Bachelor of Science Degree in Cybersecurity and Information Assurance, while preparing for the CISSP certification. Maintained a DoD Security Clearance from 01/2002 to 03/2015 when the clearance was archived due to lack of activity.

Key Career Accomplishments

- Achieving PCI-DSS Attestation of Compliance (AOC) by leading the teams responsible for resolving, remediating, mitigating, and/or establishing compensating controls of data management for over 7,500 Pen Test vulnerabilities, within a 19-day deadline.
- For a bi-annual auditing process to establish the Authority to Operate (ATO) in an Internal Audit, consistently, for a three-year period, led teams to provide evidence for over 100,000 individual settings, in less than a two week period, based on Compliance to the NIST 800-53 Framework Configuration Management controls as defined by multiple Secure Technical Implementation Guide's (STIG's).
- Reduced vulnerabilities from over 60,000 non-compliant NIST 800-53 configuration findings to zero, achieving Operational Compliance via Data Quality in a Design Program verified by Management Reporting in an enterprise structure of four locations, over 11,000 employee's serving 21.5 million people.
- Managed, led and mentored 16-member collaborate Service Desk team, providing multiple tier level technical production support in a complex war zone environment.

Key Processes

Change Management, *Project Management*, Incident Management, *Endpoint Protection*, Vulnerability and Threat Assessments, *Risk Assessment*, Remediation and Mitigation, *Information Security*, Security Documentation, *Emotional Intelligence*, Mentorship / Leadership / Negotiation Skills and *Information Management*.

Certifications

Certified Information Security Manager (CISM) *(Certification # 1840465)*

Certified Incident Handler (ECIH) *(Certification #ECC7134958062)*

Certificate of Cloud Security Knowledge (CCSK) *(Code: 5gcoMUtyn7Zc4oe7zAaRVwiQ)*

Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 *(Certification # F018-5583)*

VMware Certified Professional (VCP5-DCV) *(Code: 11374564-91D1-97DC9ED1B49B)*

Certified Identity and Access Manager (CIAM) *(Certification # 4239)*

Certified Access Management Specialist (CAMS) *(Certification # 4238)*

Microsoft Certified Technology Specialist (MCTS) Windows 7 *(Certification # A762-8759)*

CompTIA Security +; A +; Network +

Completed courseware – awaiting certification for:

Certified Cloud Security Professional *(CCSP)*

Certified Encryption Specialist *(ECES)*

Professional Experience

Bank of America
Senior Security Specialist – Policy Assessment Adherence, Dallas, TX *10/2019 - present*

Member of the GIS – Policy Assessment team specializing in application policy adherence for financial services organizational standards and regulations.

- Executing Industry Standards for financial institution applications, Kubernetes, IPSec, Docker, Security Risk Assessments and Risk Mitigation involving Data Privacy Products for Due Diligence, Business Performance, Legal and Security Compliance, Devops, Operations and cost effective product testing for the production environment.
- Using financial institution methodology to maintain compliance standards which incorporate PCI-DSS, NIST, SOX, SOC, GDPR, FFIEC and ISO standards and regulations maintaining accountability.
- Collaborating with Application Managers and their delegates, Quality Assurance (QA) and Configuration Maintenance (CM) teams to ensure required application posture is met for PAR, ASA, GIS, CSTAR and FFIEC assessments.

Alorica
Global Cyber Security Analyst, Dallas, TX 11/2018 – 03/2019

Leadership of the Information Security team specializing in Architecture and Governance, Technical Skills, Risk and Compliance. Project technical / team lead for the PCI-DSS re-certification of the AOC/ROC.

- Resolved, remediated, mitigated, and established compensating controls for 7,500+ Pen Test vulnerabilities including Root Cause analysis, intrusion detection and architectures allowing the organization to regain their AOC (Attestation of Compliance) through a clean Penetration Test and Strong Negotiation Skills.
- Developed SOC 2 Type 1 (procedures and controls) and Type 2 (proof of procedures and controls) compliance reports for Data Center networks, firewalls, routers, security systems and system configuration best practices required by American Express resulting in cessation of imposed fines.
- Led the corporate posture (with one other engineer) for Identity Access Management (IAM), Mobile Device Management and Single Sign On solutions to be fulfilled through third-party vendor contracts.
- Influenced the strategy for the Security Operation Center (SOC) to categorize and prioritize findings, implement necessary regulatory requirements and security policies and procedures.
- Forged long-term strategic networking relationships with the teams responsible for remediation, negotiation and the managerial, marketing materials to budget time and resources for Infosec.

Blue Cross Blue Shield of SC
Sr. IS Cyber Security Engineer, Dallas, TX 03/2015 – 06/2018

Creator, Leader, and Motivator of the Operational Systems Compliance (OSC) Team – effectively training and mentoring OSC staff in a strategic direction for Information Assurance practices – in accordance with corporate FCRA, GRC and HIPAA standards DISA STIG's, NIST and RMF requirements.

- Reducing 60,000+ non-compliant findings to zero through proactively influencing a strategic direction of control activities with decision making innovation in data management for Windows OS, Virtual environments, Group Policy or Active Directory.
- Encouraged internal collaboration teams to focus on vulnerability assessments, risk assessments, problems, creative solutions and organized remediation or mitigation techniques reducing impact and achieving 40% reduction in vulnerabilities.
- Created policy development and security documentation for Organizational Compliance, allowing for Enterprise Risk Management implementation. Created Business Risk Justification's, Policies and POAMs, system security plans, security controls traceability matrix, and security requirements to support the Authority to Operate (ATO) Regulatory Examination.

General Dynamics Information Technology - PACOM
Sr. System Engineer / Administrator, Oahu, HI 07/2012 – 03/2015

- Created, provisioned, influenced, and maintained enterprise-level servers and workstations for multiple world-wide classified networks for DoD in the Pacific Command achieving NIST compliance.

General Dynamics Information Technology - USACE
Sr. System Engineer / Administrator - IANO, Kabul, Afghanistan 02/2011 – 06/2012

Served as Information Assurance Security Officer (IASO), Service Desk Manager and Sr. Systems Engineer / Administrator in virtual and physical Enterprise environments in the Northern Afghanistan Region.

- Leader / Mentor / Manager of a 16-member Collaborative Enterprise Service Technologists, providing Security Requirements and Tier I, II, and III technical support.

Education

Currently completing my final year for the WGU B.S. in Cybersecurity and Information Assurance

Technical / Software

System Security Assessments/Hardening Tools:
Nessus, Tripwire, Qualys, MITRE, CVSS, STIG Viewer, Active Directory/Group Policy, Symantec Endpoint Protection/ Backup Exec, SANS 20 Critical Security Controls, Firewalls